RECORD OF INTERVIEW

The applicants would like to thank Examiner Ronald Baum for his helpful comments and suggestions during the telephone interview with the undersigned and associate attorney Wendell Peete on December 14, 2005. During the telephone interview certain aspects of novelty over the cited art were discussed.

Pursuant to 37 C.F.R. § 1.133(b), the following description is submitted as a complete written statement of the reasons presented at the interview as warranting favorable action. The following statement is intended to comply with the requirements of MPEP § 713.04 and expressly sets forth: (A) a brief description of the nature any exhibit shown or any demonstration conducted; (B) identification of the claims discussed; (C) identification of specific prior art discussed; (D) identification of the principal proposed amendments of a substantive nature discussed; (E) the general thrust of the principal arguments; and (F) a general indication of any other pertinent matters; and (G) the general results or outcome of the interview, if appropriate.

(A) No exhibits were shown or discussed.

(B) The independent claims were discussed, in particular certain aspects relating to flow-based detection of network intrusions.

(C) The *Shipley* patent (6,119,236) was discussed.

(D) No proposed amendments were officially presented or discussed, but the claim amendments presented in this paper are consistent with the discussion.

(E) The general thrust of the discussion was as set forth below in the next paragraphs.

(F) No other matters were discussed.

(G) No agreement was reached during the interview regarding the claims.

The general thrust of the discussion was that the *Shipley* patent did not disclose, teach, or suggest the claimed aspects of a flow-based detection of unauthorized network activity such as intrusions. As discussed, and among other aspects, the claimed invention(s) provide for detection of unauthorized network activity based on the

monitoring of packets between two hosts on a network that are associated with a single service, and characterizing a group of such packets as a "flow."

The examiner suggested that the claims be amended to more particularly specify what a flow is and how the flows are used in the invention. No agreement on particular claim language was reached, pending submission of a formal amendment.

The amendments herein and comments that follow are intended to be consistent with the remarks made during the interview.

In the event that the foregoing record is not considered complete and accurate, the Examiner is respectfully requested to bring any incompleteness or inaccuracy to the attention of the undersigned.

REMARKS

The Office Action has been carefully reviewed, and the following remarks herein are considered responsive thereto. Claims 1–22 are currently pending in this application. Claims 1–22 have been amended by this amendment. New claims 23–36 have been added. Of these new claims, only claim 23 is independent; the rest are dependent.

Claims 1, 4, 9, 10, 14, 17, and 20 were rejected by the Examiner under 35 U.S.C. § 102 (b) as being anticipated by U.S. Patent No. 6,119,236 to *Shipley* (hereinafter *Shipley*). Further, claims 2, 3, 5, 6–8, 11–13, 15, 16, 18, 19, 21, and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Shipley* as applied to the claims 1, 4, 10, and 17, and further in view of the patent *Vaid et al.*, U.S. Patent No. 6,502,131.

Prior to addressing the merits of the rejection specifically, applicants note the following. Specifically, and in accordance with the interview with the examiner, independent claims 1, 9, 10, and 17 have been amended to recite limitations directed to methods and systems for determining unauthorized network usage based on identified "flows." In general (e.g. claim 1 and others), these flows are derived by monitoring the exchange of packets between two hosts, and identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined characteristic. Examples of such predetermined characteristics are set forth in new dependent claim 24 and include such things as the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, the occurrence of a RESET packet, data sent by TCP and acknowledged, UDP packets that are not rejected, and local multicast or broadcast.

Other aspects (e.g. dependent claim 2) relate to displaying to a user indicia corresponding to the occurrence of particular network services observed during a monitoring period. Further aspects (e.g. dependent claim 3) relate to displaying an indication that a predetermined observed network service is in profile and observed during a monitoring period, or in profile but not observed during a monitoring period, or

is not in profile. Still further aspects (e.g. dependent claim 4) relates to generating an alarm when an observed network service is not an allowed network service. Yet further aspects (e.g. dependent claims 5–8) relate to displaying indicia indicating that an observed service is not an allowed service, building of the profile during a profile generation time, allowing editing of the profile for particular hosts, or for a block of network addresses.

Further aspects (e.g. new dependent claims 24-36) relate to determining that a flow has terminated in response to a predetermined event, e.g. when no packets are exchanged between two hosts for a predetermined amount of time, a FIN flag, RESET packets; providing an output to a utilization device; instructing a firewall to drop packets, incorporating the invention in a monitoring appliance; coupling the monitoring appliance to a network device such as router, switch, hub, tap, or network security device; and other aspects.

Support for the present independent claim amendments can be found in the specification, among other places and by way of example, at page 5, lines 21–26; page 11, line 29 to page 12, line 5; page 21, lines 15–19; page 24 (Section on Network Services); page 26, lines 3–10; and page 37 (discussion of flow charts). No new matter has been added by this amendment.

An indication of support for the various new dependent claims is recited specifically in detail below in a separate section.

35 U.S.C. § 102 (b) REJECTION UNDER *SHIPLEY*

Claims 1, 4, 9, 10, 14, 17, and 20 were rejected under 35 U.S.C. § 102(b) as being anticipated by *Shipley*. Claims 1, 9, 10, and 17 of this group are independent claims. In view of the amendments to these claims, it is believed that the claims are not anticipated – without admitting that the claims were ever really anticipated. Accordingly, the amendments made herein are for clarity in understanding the claimed subject matter.

The examiner cited the *Shipley* patent as showing the various originally-recited steps of capturing packet header information, determining valid connections or data flows, determining hosts on the network that act as a client and server for each valid connection, determining network services used by every host in a group of hosts, etc. (Office Action, page 2.) The examiner cited alleged teachings in *Shipley* as suggesting the limitation of claim 4 relating to storing an allowed network services profile, comparing allowed network services with observed network services, generating an alarm, etc. (Office Action, page 3.)

In view of the amendments to the claims, and the following comments about the *Shipley* patent, it is requested that the rejection be reconsidered and withdrawn.

The *Shipley* patent relates to an intelligent network security device (INSD) that is configured to operate within a local area network ("LAN"), wherein the LAN is in communication with the Internet via a firewall. Within the internal boundaries of the firewall, the INSD monitors the LAN's communications that travel through the firewall looking for specific codes and patterns of behavior. (*Shipley*, Abstract.) The *Shipley* INSD assigns a value to any perceived attempted network security breach. Based upon the attempted security breach assigned value, the INSD instructs a firewall to take any of a prescribed plurality of actions.

As to the *Shipley* method of looking for "specific codes," it is apparent that such analysis requires inspection of data in each packet known to be indicative of security breach attempts. (*Shipley*, col. 5, lines 60–62). This is clearly not a flow-based methodology.

As to the *Shipley* method of looking for "known patterns," this methodology is not clearly spelled out in the patent. These "patterns of activity" (*Shipley* col. 6, line 9–14) are only generally described; very few specific examples are given aside from the very general description of an "ordered attempt to access each machine on a network" (col. 6, lines 17–18), or "access ports which do not exist" (col. 6, lines 32–33), or "access a port which is ... not used" (col. 6, lines 40–43).

However, there is clearly no teaching of using a flow-based approach to detecting unauthorized activity, e.g. in the form of out-of-profile services, and no specific analytical method described at all. Indeed, *Shipley* clearly asserts that "in order for the 'look for known patterns' operation 36 to be successful, the INSD 10 might require some knowledge of the configuration of the LAN 12 ..." (Col. 6, lines 57–60). This does not teach or suggest anything relating to use of a flow-based detection approach.

For the reasons that will be explained, the flow-based profiling approach as recited in the claims of the present application is patentably different from the specific code- and pattern-based approach in the *Shipley* patent.

More specifically, *Shipley* initially describes the INSD as monitoring all Ethernet packets that are coming or going through the firewall in a "receive input" operation. Following the "receive input" operation, the INSD performs a "look for known code" operation and a "look for known pattern" operation. (*Shipley*, FIG. 2.) Within the "look for known code" operation, the INSD makes a comparison between the data that is contained within each Ethernet packet to data that is known to be indicative of security breach attempts.

As described in *Shipley*, the "look for known code" operation is performed simultaneously with the "look for known patterns" operation. In the "look for known patterns" operation, the INSD examines the patterns of activity of the communications on the LAN. This aspect is described within *Shipley* as requiring that the INSD retain certain data for a limited amount of time in order to identify and examine the patterns of communicative activity within the LAN.

Following the completion of the "look for known patterns" operation and the "look for known code" operation, the INSD in *Shipley* performs an "assign weight to breach" and "react" operation, respectively. The specific function of the "assign weight to breach" operation is to provide a value that is based upon the average of various factors that are used to ascertain if there is a perceived attempted network security breach. If the system determines that there is an attempted network breach, then

following the "assign weight to breach operation," the "react" operation is performed. In the "react" operation, the INSD sends a control signal to the firewall via a serial cable. The control signal directs the firewall to perform any of a number of prescribed actions that are based upon the value that has been determined in the "assign weight to breach" operation. (See e.g. *Shipley*, col. 7, lines 50–57.)

In contrast to *Shipley*, the claims in this application (as amended, and in certain aspects) describe systems and methods for determining unauthorized activity based on determining "flows" and services associated with flows – not on known codes, and not as regards known patterns in the way described in *Shipley*. Further still, the claims generally involve determining whether such services are appropriate relative to a profile maintained for a particular host. As described amply in the specification, a flow (for some claims, e.g. claim 1, as amended) is identified by monitoring the exchange of packets between two hosts, and identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and characterized by a predetermined characteristic. According to another aspect, claim 1 recites storing information associating a service that is associated with an identified flow with at least one of the hosts that is associated with the identified flow. This service is an "observed service."

Further still, claim 1 recites determining if an observed service associated with a particular host is out of profile by comparing the service to a prestored allowed network services profile for the particular host. Finally, claim 1 recites, in response to determination that an observed service associated with a particular host is out of profile, providing an output indicating that the observed service is out of profile. Such steps are not disclosed, taught, or suggested in *Shipley*.

Shipley does not disclose, teach or suggest a method of determining whether usage on a network is unauthorized involving monitoring packets exchanged between two hosts on the data communication network, and then identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a

single service and has a predetermined characteristic. Nor does *Shipley* disclose, teach or suggest storing information associating an observed service with a determined flow, or determining if that observed service is appropriate for a particular host, given a stored profile for that host (generally stated).

In *Shipley*, a decision to issue an alarm (or signal a firewall to block certain packets) is entirely based upon a value that has been assigned to a "breach" that can be based upon a singular event that can be associated with a "look for known code" operation and/or a "look for known pattern" operation. The "assign weight to breach" operation provides a value based upon the average of various factors that are used to ascertain if there is a perceived attempted network security breach. This bears no relation to the monitoring of packets and identifying a flow based on a predetermined plurality of packets that relate to a single service, and/or by a predetermined characteristic.

Claim 9, as amended, is also directed to the notion of monitoring packets, identifying a flow as corresponding to a predetermined plurality of packets exchanged between two hosts that relate to a single service, storing information about an observed service associated with a flow in association with a host, and determining if the observed service is authorized. However, claim 9 differs by reciting the step of determining an allowed network services profile comprising information indicating particular network services that are authorized for use by each one of a plurality of hosts a predefined group of hosts. Claim 9 also recites the step of generating an alarm in response to determination that an observed network service for a particular host in the group of hosts is not included in the allowed network services profile. This is also not disclosed, taught, or suggested in *Shipley*.

Claim 10, as amended, is also directed to the notion of monitoring packets, identifying a flow in the manner recited, storing information about an observed service associated with a flow in association with a host, and determining if the observed service is authorized. However, claim 10 differs by also reciting the step of storing an allowed network services port profile for each one of a plurality of hosts in a predefined host

group, said profile including information identifying port numbers that are authorized for use by each host in the host group. Further, claim 10 recites the step of determining the port numbers of observed network services used by each host in the predefined host group for each identified flow, and comparing the allowed network services port profile with observed network service port numbers. Further, claim 10 also recites the step of generating an alarm when an observed network service port number is not included in the allowed network service port profile. This is also not disclosed, taught, or suggested in *Shipley*.

Claim 17, as amended, is directed to a system for determining unauthorized usage of a network, which comprises a monitoring device that includes a processor that is operative to carry out certain recited steps. Those steps include monitoring packets, identifying a flow (in the manner recited), storing information about an observed service associated with a flow in association with a host, determining if the observed service is authorized, and in response to determination that an observed service associated with a particular host is out of profile, providing an output indicating that the observed service is out of profile. Such as system is not disclosed, taught, or suggested in *Shipley*.

Therefore, in view of the above remarks, the Applicant believe that all aspects of the Section 102(b) rejection based on *Shipley* have been addressed, and respectfully requests that the rejection of independent claims 1, 9, 10, and 17 be withdrawn. Because the remaining claims rejected on these grounds are dependent claims and add further limitations, it is requested that the rejection of these claims also be withdrawn.

35 U.S.C. § 103 (a) REJECTION UNDER *SHIPLEY* IN VIEW OF *VAID ET AL.*

Claims 2, 3, 5, 6–8, 11–13, 15, 16, 18, 19, 21, and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Shipley*, as applied to the rejection of the claims above, and further in view of the U.S. Patent No. 6,502,131 to *Vaid et al.* The examiner indicated that the teachings of *Shipley* suggest the base claims limitations, without explicitly teaching features such as displaying indicia, building and editing a

network profile, etc. *Vaid et al.* was cited as teaching the display of indicia, security aspects, etc. (Office Action, page 11.) The examiner asserted that it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the *Shipley* network security device and method of firewall control with the teachings of *Vaid et al.* with its alleged firewall/network gateway node directory enabled policy management tool for intelligent traffic management, in order to provide firewall configuration and efficient control thereof.

All of the claims rejected on these grounds are dependent claims. In view of the amendments to the respective independent claims, it is submitted that these dependent claims are not obvious.

The *Vaid et al.* patent is directed to a "directory enabled policy management tool for intelligent traffic management." It is not directed to network security or determining whether use is authorized or not – it merely provides a view as to the nature of the traffic on the network. While there is mention of "flows" (e.g. the FAIR module (Flow Analysis and Intelligent Regulation, col. 13, line 57), these flows relate to traffic classes, and setting policies to control traffic flows (see col. 17, lines 1–22). Also, while there is mention of "services" (see col. 18, line 37), there is no teaching about identifying a flow corresponding to a plurality of exchanged packets that relate to single service, as recited in the base claims, and identifying a service associated with that flow, and then determining whether that service is in profile or out of profile for a host.

The policy management tool in *Vaid et al.* is clearly directed to showing traffic classes and utilization of bandwidth and other parameters for such determined traffic classes. See e.g. FIG. 13 with its display of "class bandwidth" for various types of traffic such as FTP_IN, HTTP_IN, etc. It does not disclose or teach indicia corresponding to the occurrence of a particular service for purposes of determining whether such services are considered in profile or out of profile, as recited in claim 2, as amended.

Similar observations are applicable for the other dependent claims – *Vaid et al.* does not teach anything about display of indicia that particular observed services are in

profile and observed, in profile but not observed, or out of profile (claims 3, 5, as amended). Nor does it teach anything about generating an alarm when an observed service is not an allowed service (claim 4, as amended). Nor does it teach anything about building up an allowed network services profile based on services observed during a profile generation time (claim 6, as amended). Nor does it teach anything about allowing user editing of an allowed network services profile (claim 7, as amended), as the "allowed network services profile" language should be interpreted. Nor does it teach anything about editing an allowed network services profile for a block of addresses (claim 8, as amended).

Similar observations apply to dependent claims 11–13, 15, 16, 18, 19, 21, and 22. The remarks above are equally applicable to these dependent claims. For the same reasons, it is requested that the rejection be withdrawn.

Furthermore, under the doctrine of *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. Claims 2, 3, 5, 6–8, 11–13, 15, 16, 18, 19, 21, and 22 should be allowable on this basis, as well.

NEW CLAIMS

New claims 23–36 are presented for entry. These new claims raise no new issues not already considered by the examiner, are supported in the specification (as will be shown), are not new matter, and are entered to provide additional protection for the claimed inventions especially as regards the doctrine of claim differentiation.

New independent 23 is a system claim that recites elements of a processor that is operative to carry out the flow-based / services port profiling, including maintaining a flow data structure and a host data structure, a memory for storing the data structures, and a network interface coupled to the processor operative to receive packets on the data communication network. Support is found in the specification on page 26, line 12 through page 28, line 28, and elsewhere.

New dependent claims 24–36 qualify various independent claims in multiple dependent claim format as permitted under 36 C.F.R. 1.75(c).

New dependent claim 24 recites that the predetermined event that delimits a flow can be elapse of a predetermined time, a FIN flag, predetermined characteristics of traffic, a RESET packet; data sent by TCP and acknowledged, UDP packets that are not rejected, and local multicast or broadcast.. Support is found in the specification on page 13, line 12; page 22, line 21; page 23, lines 5-9; other discussion on page 23; page 25, lines 6–9, 14; among other places.

New dependent claim 25 recites that the step of providing an output or alarm comprises the step of communicating a message to a firewall to drop packets going to or from the particular host. Support is found in the specification on page 34, lines 17–22, among other places.

New dependent claim 26 recites that the output or alarm is a notification to a network administrator. Support is found in the specification on page 34, lines 12–17, among other places.

New dependent claim 27 recites that the output or alarm is provided to a utilization component selected from the group comprising: network security device, email, SNMP trap message, beeper, cellphone, firewall, network monitor, user interface display to an operator. Support is found in the specification on page 34, lines 12–22, among other places.

New dependent claim 28 recites that the single service comprises a port number remaining constant for a plurality of packets. Support is found in the incorporated specification Application No. 10/000,396 on page 5, lines 10–12, among other places.

New dependent claim 29 recites that the steps are carried out in a monitoring appliance. Support is found in the specification on page 12, line 19, among other places.

New dependent claim 30 recites that the monitoring appliance monitors communications among inside hosts and outside hosts. Support is found in the specification on page 12, line 21–23, among other places.

New dependent claim 31 recites that the monitoring appliance is coupled to a network device. Support is found in the specification on page 12, lines 19–20, among other places.

New dependent claim 32 recites that the network device is selected from the group comprising: router, switch, hub, tap. Support is found in the specification on page 12, line 21, among other places.

New dependent claim 33 recites that the network device is a network security device. Support is found in the specification on page, line 20, among other places.

New dependent claim 34 recites that the monitoring of packets comprises monitoring packet header information only. Support is found in the specification on page 30, line 8, among other places.

New dependent claim 35 recites that the unauthorized use is from an inside address or from an outside address. Support is found in the specification on page 34, lines 3-4, among other places.

New dependent claim 36 recited that a service is associated with an identified flow in response to initiation of communications between the two hosts. Support is found on the specification page 16, line 21-25; page 24, line 5 through page 25, line 5, among other places. This claim is added to provide additional protection for the invention by way of the doctrine of claim differentiation, so that the record is clear that the association of a service with a flow need not occur at any particular time.

* * * * *

CONCLUSION

For the foregoing reasons, it is submitted that all claims are believed novel, nonobvious, fully supported, and should be allowable. The foregoing is submitted as a full and complete response to the Office Action mailed September 29, 2005 and is believed to place all claims in the application in condition for allowance. Accordingly, it

is respectfully submitted that this application be allowed and that a Notice of Allowance be issued. If the Examiner believes that a telephone conference with the Applicant's attorneys would be advantageous to the disposition of this case then the Examiner is encouraged to telephone the undersigned.

Credit Card Payment Form PTO-2038 in the amount of $2,155.00 is enclosed to cover the fees for two-month extension of time ($225) and fee for extra claims and multiple dependent claims ($1,930).

Respectfully submitted,

Dated: January 27, 2006

By: John R. Harris
Reg. No. 30,388
Attorneys for Applicant

MORRIS, MANNING & MARTIN, LLP
3343 Peachtree Rd. NE
1600 Atlanta Financial Center
Atlanta, GA 30326
(404) 233-7000
(404) 365-9532 – fax

Docket: 10775-36791